Report 479: Australian Government Security Arrangements

Inquiry based on Auditor-General’s reports 38 and 43 (2017-18)

Joint Committee of Public Accounts and Audit
# Contents

Membership of the Committee ................................................................. v
List of Recommendations ......................................................................... vii

## The Report

1 **Executive Summary** ................................................................................. 1
   Mitigating Insider Threats through Personnel Security ................................. 1
   Domestic Passenger Screening – FollowUp ................................................ 2

2 **Mitigating Insider Threats through Personnel Security** ......................... 5
   Committee conclusions and recommendations ............................................. 5
      Entity compliance with personnel security requirements ........................ 6
      Information control .................................................................................. 10
   Review of evidence ...................................................................................... 15
      Previous ANAO report ............................................................................ 15
      Clearance rates ....................................................................................... 16
      ICT and documentation issues ................................................................. 17

3 **Domestic Passenger Screening - Follow-Up** ........................................... 25
   Committee conclusions and recommendations .......................................... 25
   Review of evidence ...................................................................................... 31
      Compliance monitoring .......................................................................... 32
      Learning and development ..................................................................... 36
      Performance monitoring and reporting ................................................. 41
Appendix A. Terms of Reference and JCPAA Role ...........................................45
Appendix B. ANAO Conclusions and Recommendations .................................47
Appendix C. Submissions ..............................................................................53
Appendix D. Public Hearings ........................................................................55
Membership of the Committee

Chair
Senator Dean Smith

Deputy Chair
Mr Julian Hill MP

Members
Ms Nicolle Flint MP
Mr Andrew Gee MP (to 25 January 2019)
Mr Andrew Laming MP
Senator Chris Ketter
Senator Jenny McAllister
Ms Madeleine King MP
Senator the Hon Eric Abetz
Mrs Nola Marino MP
Senator Rex Patrick
Senator Steve Martin
Mr Andrew Hastie MP
Ms Gai Brodtmann MP

Mr Ross Hart MP

Committee Secretariat

Joel Bateman, Committee Secretary (from 4/2/19)
Susan Cardell, Committee Secretary (to 1/2/19)
Anthony Overs, Inquiry Secretary
Klara Fay, Senior Research Officer
Irena Korenevski, Graduate
Tamara Palmer, Office Manager
List of Recommendations

Recommendation 1

2.18 The Committee recommends that the Auditor-General consider conducting a number of additional audits of Australian Government entities focusing on their performance against Protective Security Policy Framework requirements and recommended practices.

Recommendation 2

2.27 The Committee recommends that each of the five entities scrutinised in Audit Report 38 (2017-18) provide a progress report to the Committee, within three months and with an update every twelve months, on their implementation of the recommendations from the Audit Report and the status of their compliance with the Protective Security Policy Framework.

Recommendation 3

2.33 The Committee recommends that the Department of Defence expedite the ICT2270 Vetting Transformation project and provide to the Committee a progress report and updated timeline on implementation of the replacement ICT system.

Recommendation 4

2.43 The Committee recommends that the Department of Defence establish extra safeguards and quality control measures to ensure that no incidents of sensitive data loss occur prior to operational capability of the new vetting case management system.
Recommendation 5

2.49 The Committee recommends that the Department of Defence prepare a full business case to consider the current and alternative service delivery models, taking account of projected future demand for vetting, the costs, benefits and risks of various approaches, and provide the findings of this to the Committee within 12 months.

Recommendation 6

3.10 The Committee recommends that the Australian National Audit Office consider conducting a follow-up audit in 2019-20, focusing on the department’s implementation of eight agreed ANAO recommendations and considering the department’s entire compliance program.

Recommendation 7

3.14 The Committee recommends that the Department of Home Affairs:

- gather an appropriate baseline data set prior to the implementation of Regulatory Management System upgrade in the first quarter of 2019;

- monitor and review the outcomes of the upgrade against the baseline data set, particularly whether data quality is improving; and

- either prioritise an additional upgrade to the Regulatory Management System in order to establish an efficient and effective reporting function, or prioritise the development of the data product suite (as was approved on 10 November 2017) in order to address the limitations to data quality and performance reporting identified in the ANAO report.

Recommendation 8

3.16 The Committee recommends that the Department of Home Affairs report back to the Committee on progress in the implementation of the compliance and enforcement framework in detail, including objectives, timeframes, milestones, lines of responsibility, performance measures, evaluation and reporting arrangements, and further information on the centralised case management system.
Recommendation 9

3.18  The Committee recommends that the Department of Home Affairs report back to the Committee on training undertaken by staff in relation to the Regulatory Management System, and whether improvements to data quality, reliability and accuracy are being measured and achieved.

Recommendation 10

3.23  The Committee recommends that in relation to the learning and development framework, the Department of Home Affairs:

- establish a formal monitoring mechanism to provide assurance that all ongoing and new operational staff have undertaken the required qualifications and re-accreditation; and

- consider using the results of the training needs analysis from February 2017 as baseline data in the monitoring and evaluation of the learning and development framework.

Recommendation 11

3.25  The Committee recommends that the Department of Home Affairs report back to the Committee on the implementation of performance measures for passenger screening, including:

- the outcomes of the trial implementation period of performance measures with industry participants; and

- the department’s target date for full implementation of performance measures.
1. Executive Summary

1.1 The Joint Committee of Public Accounts and Audit (JCPAA) inquiry into Australian Government Security Arrangements was based on the following Australian National Audit Office (ANAO) reports:

- No. 38 (2017-18), Mitigating Insider Threats through Personnel Security
- No. 43 (2017-18), Domestic Passenger Screening – Follow-Up

Mitigating Insider Threats through Personnel Security

1.2 Personnel security, a component of the Australian Government’s Protective Security Policy Framework (PSPF), aims to mitigate insider threats by assessing the eligibility and suitability of individuals accessing government resources. The Australian Government Security Vetting Agency (AGSVA), based in the Department of Defence, administers personnel security vetting.

1.3 A previous audit concluded that the performance of centralised vetting had been mixed, and improved efficiency and cost effectiveness were not evident.

1.4 This audit aimed to examine vetting performance and the implementation of more recent personnel security reforms.

1.5 The Audit Report found that the effectiveness of personnel security arrangements was reduced as AGSVA had not implemented the Australian Government’s policy direction to share identified personnel security risk information with client entities.

1.6 The Audit Report examined the development and implementation of personnel security plans, policies and procedures across several government entities, finding that compliance varied greatly.
1.7 The Committee noted that the five entities examined had accepted the Audit Report recommendations, with implementation mostly complete or well underway. The Committee recommends that the five audited entities report back to the JCPAA on the implementation of the recommendations from the Audit Report and compliance with the PSPF.

1.8 Considering that AGSVA administers personnel security vetting services for more than 150 Commonwealth and state government agencies, the sample of five entities examined in the Audit Report may not be representative of what is actually happening across all agencies or entities. The Committee recommends that the Auditor-General consider further audits into the performance of a significant proportion of the 150 Australian Government agencies against the PSPF requirements.

1.9 Audit Report 38 identified significant issues concerning AGSVA’s information systems. AGSVA stated that the current system does not meet its business needs. Although the development and implementation of a replacement system has begun, there is still a substantial wait for any initial operating capability and a fully operational system is some five years away. Inefficient processes and poor data quality, as well as the extensive exchange of information outside of a secure environment, will continue until the new system is in place. The Committee recommends that the Department of Defence move to have a new vetting case management system in place as soon as possible. The Committee also recommends that Defence provide a progress report and timeline for the implementation of the new vetting case management system.

Domestic Passenger Screening – Follow-Up

1.10 The Department of Home Affairs undertakes domestic passenger screening in order to prevent prohibited items such as weapons and explosives being carried onto aircrafts. Screening needs to be conducted efficiently and must meet legislated and regulatory requirements.¹

1.11 The ANAO previously tabled Auditor-General Report No. 5 (2016-17), Passenger Screening at Domestic Airports on 31 August 2016. This audit made five recommendations aimed at improving the department’s (then, the Department of Infrastructure and Regional Development) regulatory performance. In 2017-18, the ANAO undertook a follow-up audit to examine

the extent to which the Department of Home Affairs (the department) had implemented the five recommendations of the previous audit.

1.12 The follow-up audit concluded that as at March 2018, the department had implemented one and partially implemented four of the five recommendations from the previous audit. The ANAO stated that although the department had made progress, it was not yet ‘well placed to provide assurance that passenger screening is effective and that screening authorities comply with the Regulations’.²

1.13 The department has acknowledged that the compliance data in its information technology systems has been challenging and that ‘the ease of use of the system is not perfect’.³ Although the department has made improvements, the Committee’s view is that the recurrent issues around quality of data and the use of manual processes for analysis and reporting will continue to impact on the department’s ability to provide assurance that robust data and efficient reporting is informing passenger screening and compliance activities.

1.14 The department has commenced implementation of the compliance and enforcement framework with an initial focus on staff capability training. The Committee noted the three-year timeframe for implementation, which may be extended by a further 12 to 24 months, and recommended that the department report back to the Committee with more detailed information regarding the implementation timeframes and milestones.

1.15 The department commenced delivering the learning and development program in February 2018, with all staff to be appropriately qualified by the start of 2019. The Committee noted concerns regarding the monitoring and evaluation component and the baseline data available for the learning and development framework, and subsequently made two recommendations.

1.16 The Committee is concerned by the department’s slow progress in developing and implementing performance measures for passenger screening.⁴ The department’s advice at the September 2018 public hearing regarding the timeframe for implementation is different to the timeframe initially reported by the ANAO, further undermining the Committee’s

³ Mr Angus Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 2.
⁴ ANAO Report No. 43 (2017-18), p. 33. As noted by the ANAO, numerous reviews since 2002 have noted the need for the department to develop and implement performance measures.
confidence that performance measures will be implemented in a timely manner. The Committee has recommended that the department report back on the implementation timeframes.

5 ANAO Report No. 43 (2017-18), p. 34; Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, pp. 7-8. The ANAO reported that full implementation of performance measures was scheduled to commence on 1 July 2018, following a trial period commencing in March 2018. Comparatively, the department later advised that there was no expected implementation date, and the trial period began in May 2018 and is scheduled to conclude in October 2018.
2. Mitigating Insider Threats through Personnel Security

2.1 This chapter sets out the Committee’s findings in relation to the implementation of recommendations from the Australian National Audit Office (ANAO) Report No. 38 (2017-18), Mitigating Insider Threats through Personnel Security. It comprises the following sections:

- Committee conclusions and recommendations
- Review of evidence

Committee conclusions and recommendations

2.2 The Australian Government’s Protective Security Policy Framework (PSPF) outlines a suite of requirements and recommendations to assist government entities to protect their people, information and assets. Personnel security, a component of the PSPF, aims to provide a level of assurance as to the eligibility and suitability of individuals accessing government resources. This is achieved through measures such as conducting employment screening and security vetting, managing the ongoing suitability of personnel and taking appropriate actions when personnel leave.¹

2.3 In 2014, the Attorney-General announced reforms to the PSPF to mitigate insider threats by requiring more active management of personnel risks and greater information sharing between entities. Further PSPF reforms were being considered by the Australian Government at the time of the audit.²

2.4 The Australian Government Security Vetting Agency (AGSVRA) was established within the Department of Defence (Defence) in October 2010 to administer security vetting on behalf of most government entities.\(^3\) Centralised vetting was expected to result in:

- a single security clearance for each employee or contractor, recognised across government entities;
- a more efficient and cost-effective vetting service; and
- cost savings of $5.3 million per year.\(^4\)

2.5 A previous audit (ANAO Audit Report No.45 of 2014-15 *Central Administration of Security Vetting*) concluded that the performance of centralised vetting had been mixed and expectations of improved efficiency and cost effectiveness had not been realised.\(^5\)

2.6 The ANAO chose to undertake this audit in 2017-18 because effective personnel security arrangements underpin the protection of the Australian Government’s people, information and assets, and the previous audit had identified deficiencies in AGSVA’s performance. In addition, the Audit Report explains that the 2014 personnel security reforms occurred after fieldwork for the previous audit had been completed, so there was an opportunity to review the implementation of these reforms by AGSVA and other government entities.\(^6\)

**Entity compliance with personnel security requirements**

2.7 The Audit Report found that four of the five entities\(^7\) examined had plans, policies and procedures in place for personnel security. However, in some cases these documents had not been updated to reflect 2014 revisions to PSPF personnel security requirements. In addition, the Audit Report found

---

\(^3\) ANAO, Report No. 38 (2017-18), p. 7; government entities that are exempt are the five intelligence and law enforcement agencies.


\(^7\) The five entities were:
  - Attorney-General’s Department (AGD)
  - Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)
  - Australian Securities and Investments Commission (ASIC)
  - Department of Home Affairs (Home Affairs)
  - Digital Transformation Agency (DTA).
that there was limited evidence of entities undertaking personnel security risk assessments to inform their plans, policies and procedures.\(^8\)

2.8 Table 3.1 of the Audit Report provided a compelling visual summary of the performance of the five entities against the PSPF requirements and recommended practices, with a focus on whether entities are effectively planning, developing policies and procedures and undertaking risk assessment for personnel security.\(^9\) The table is reproduced as Table 2.1 over the page.

2.9 The Committee was disappointed to learn that the Department of Home Affairs, a larger operational agency with almost 14,000 employees across the country and overseas, had fully met only two of the six criteria.

2.10 The Committee was equally disappointed to learn that the agency with the lead in development of protective security policy, the Attorney-General’s Department (AGD), had met none of the six criteria (having mostly met three criteria and partly met three criteria).

**Immediate action**

2.11 Table 3.1 of the Audit Report showed that the Digital Transformation Agency (DTA) had not met four criteria and had only partly met two criteria. The Committee was concerned that the DTA, admittedly a relatively new entity established in June 2015, had not finalised a protective security plan, policies or a risk assessment. The Audit Report recommended that immediate action be taken by the DTA to comply with the PSPF requirements.\(^10\)

---


2.13 As per usual ANAO processes, each entity was provided the opportunity to comment on and respond to recommendations in the draft Audit Report prior to its publication.

2.14 In March 2018, the DTA informed the Auditor-General that the agency agreed with the five proposed recommendations, which were subsequently published in the Audit Report in May. DTA made a commitment to have the recommendations implemented by 31 July. At the Committee’s public
hearing for the inquiry on 17 August, the DTA representative informed the Committee that the agency is now compliant with the PSPF.\textsuperscript{11}

2.15 The Committee was concerned as to what state the DTA would be in, regarding PSPF compliance, if it were not subject to the audit.

2.16 The Committee understands that the five entities examined during the audit were selected to provide coverage of a variety of entity functions, locations and sizes.\textsuperscript{12} The Audit Report points out that AGSVA conducts security vetting services for more than 150 Australian Government entities, as well as state and territory entities.\textsuperscript{13} The Committee is concerned that the poor compliance results of the five entities subject to the audit may be indicative of poor compliance throughout other government entities or agencies.

2.17 The Committee is cognisant of the fact that auditing every agency is not possible or practical; however, the Committee considers that additional scrutiny of a larger proportion of Australian Government entities may be required to test if broad scale PSPF compliance is being achieved.

**Recommendation 1**

2.18 The Committee recommends that the Auditor-General consider conducting a number of additional audits of Australian Government entities focusing on their performance against Protective Security Policy Framework requirements and recommended practices.

2.19 Each of the five entities examined during the audit reported their progress in meeting the Audit Report recommendations through submissions to the inquiry, and through evidence at the public hearing.

2.20 Progress was mixed, with some entities yet to complete significant tasks.

2.21 The DTA representative reported that the agency was now compliant with all five recommendations, explaining that although the agency was behind schedule, the security personnel and overall security plan were endorsed and signed off on 14 August 2018, three days prior to the public hearing.\textsuperscript{14}

\textsuperscript{11} Mr George-Philip de Wet, Digital Transformation Agency, Committee Hansard, Canberra, 17 August 2018, p. 6.


\textsuperscript{14} Mr Philip de Wet, Digital Transformation Agency, Committee Hansard, Canberra, 17 August 2018, p. 6.
2.22 The AGD representative stated that recommendation seven was complete and recommendations six and eight were well advanced with completion expected by December 2018.\(^{15}\)

2.23 The ASIC representative reported that recommendations seven and eight were complete, with recommendation six to be complete by December 2018.\(^{16}\)

2.24 The ARPANSA representative reported that recommendation seven had been met and that compliance with recommendation eight would be met by the end of 2018.\(^{17}\)

2.25 The Department of Home Affairs representative reported that addressing recommendations six and eight was well advanced and should be complete by November 2018.\(^{18}\)

2.26 The Committee expects each entity to implement all recommendations in a timely fashion.

**Recommendation 2**

2.27 The Committee recommends that each of the five entities scrutinised in Audit Report 38 (2017-18) provide a progress report to the Committee, within three months and with an update every twelve months, on their implementation of the recommendations from the Audit Report and the status of their compliance with the Protective Security Policy Framework.

**Information control**

*Information and communications technology (ICT)*

2.28 The Audit Report found that AGSVA’s information systems do not meet its business needs, resulting in inefficient processes, poor data quality, and

---

\(^{15}\) Ms. Sarah Chidgey, Deputy Secretary, Attorney-General’s Department, *Committee Hansard*, Canberra, 17 August 2018, p. 6.

\(^{16}\) Mr Carlos Iglesias, Chief of Operations, Australian Securities and Investments Commission, *Committee Hansard*, Canberra, 17 August 2018, pp. 6-7.

\(^{17}\) Dr Gillian Hirth, Deputy Chief Executive Officer, Australian Radiation Protection and Nuclear Safety Authority, *Committee Hansard*, Canberra, 17 August 2018, p. 7.

\(^{18}\) Mr Mark Brown, First Assistant Secretary, Department of Home Affairs, *Committee Hansard*, Canberra, 17 August 2018, p. 7.
integrity issues. Ano Audit Report No.45 (2014–15) also identified shortcomings in AGSVA’s ICT systems.20

2.29 Issues identified in the existing vetting case management system include:

- significant data quality issues;
- completion of all vetting tasks is not enforced;
- lack of ability to measure performance;
- vetting service contractors do not have access; and
- potentially sensitive information is communicated outside of Defence’s secure ICT environment.21

2.30 Defence has commenced the ICT2270 Vetting Transformation project to develop a replacement system. The project is currently in the initial scoping and approval stages. Information provided in the Audit Report stated that delivery of an initial operating capability was expected in late 2020, however the system would not be fully operational until 2023.22

2.31 The Defence representative stated that, ‘in terms of the case management and the foundational system being more secure, more digitised and more automated, the plan is to deliver that capability in late 2020’.23

2.32 The Committee is of the opinion that the development and implementation of the replacement ICT system to significantly reduce or eliminate vetting process flaws should be a very high priority for the Department of Defence.

Recommendation 3

2.33 The Committee recommends that the Department of Defence expedite the ICT2270 Vetting Transformation project and provide to the Committee a progress report and updated timeline on implementation of the replacement ICT system.

Handling of documentation

23 Mr Daniel Fortune, Assistant Secretary Vetting, Department of Defence, Committee Hansard, Canberra, 17 August 2018, p. 4.
2.34 Security clearance records are currently communicated via both mail and email, with contractors accumulating a considerable volume of hard-copy and electronic information, over which AGSVA has limited oversight.\textsuperscript{24}

2.35 AGSVA’s Industry Vetting Panel deed requires contractors to comply with Defence’s information security policies. However, AGSVA’s internal quality assurance reviews of contractors have identified that these requirements were frequently not adhered to.\textsuperscript{25} The risks of non-compliance and costs of monitoring compliance are exacerbated by the nature of Defence’s outsourcing arrangements which now have 22 individual contractors\textsuperscript{26} undertaking 85 per cent of all clearances including an increasing number of the positive vetting.\textsuperscript{27} This complexity is exacerbated by the deficient IT system which contractors cannot access.\textsuperscript{28}

2.36 The Committee noted that the positive vetting process deals with very detailed and highly personal information that typically covers a long history for the individuals concerned.

2.37 Despite questioning, the Committee remains unclear as to what information is being kept by the IVP companies after 90 days and is concerned about the risk of remaining disaggregated information being reconstructed in the event of a cyber attack.

2.38 The Committee also raised concerns about the handling of sensitive documents via email, mail and courier services during the clearance process. Despite reassurances from Defence, the Committee remains concerned about the safe handling of sensitive documents prior to the establishment of the new case management system.

\textit{Contractor assurance}

2.39 The Committee was concerned about the foreign ownership and control of some of the vetting entities contracted by Defence.

2.40 Defence explained that any vetting entity employee that is conducting security clearances, as well as any non-vetting staff that handle or access any

\textsuperscript{25} ANAO, Report No. 38 (2017-18), p. 41.
\textsuperscript{26} Mr Fortune, Department of Defence, \textit{Committee Hansard}, Canberra, 17 August 2018, p. 3.
\textsuperscript{27} Mr Fortune, Department of Defence, \textit{Committee Hansard}, Canberra, 17 August 2018, p. 2.
\textsuperscript{28} ANAO, Report No. 38 (2017-18), pp. 40-41.
official material, must hold an Australian Government security clearance.\textsuperscript{29} Defence noted that this was a requirement as part of the Foreign Ownership, Control and Influence (FOCI) assessment which all members of the Defence Industry Security Program (DISP) are required to undergo.\textsuperscript{30}

2.41 Defence stated that all industry vetting officers working on positive vetting clearances are Australian citizens, and confirmed that, at the time of the second public hearing, there were no vetting officers working under a citizenship eligibility waiver.\textsuperscript{31} Defence also confirmed that only ‘one company providing positive vetting services for Defence had a UK-national, Australian resident Director’, and that ‘no other companies providing positive vetting services list foreign directors’.\textsuperscript{32}

2.42 Despite this assurance, the Committee is concerned that some vetting entities may have managers or company owners that are not Australian citizens who may have access to any some or all data handled by that entity.

**Recommendation 4**

2.43 The Committee recommends that the Department of Defence establish extra safeguards and quality control measures to ensure that no incidents of sensitive data loss occur prior to operational capability of the new vetting case management system.

**Costs and benefits of the current approach**

2.44 The Committee notes that 85 per cent of all clearances are now undertaken by ‘industry partners’ – private contractors – as a result of rapid outsourcing.\textsuperscript{33} The Department of Defence advised that all procurement is managed in accordance with Defence and Commonwealth Procurement Rules.\textsuperscript{34}

2.45 During the public inquiry questions were raised regarding the costs, benefits and risks arising as a result of the outsourcing that has now occurred. Committee members were interested to understand if a cost-benefit

\textsuperscript{29} Mr Fortune, Department of Defence, *Committee Hansard*, Canberra, 12 February 2019, p. 7.

\textsuperscript{30} Department of Defence, *submission 6.3*, p. 5.

\textsuperscript{31} Department of Defence, *submission 6.3*, p. 10.

\textsuperscript{32} Department of Defence, *submission 6.3*, p. 6.

\textsuperscript{33} Mr Fortune, Department of Defence, *Committee Hansard*, Canberra, 17 August 2018, p. 15.

\textsuperscript{34} Mr Fortune, Department of Defence, *Committee Hansard*, Canberra, 17 August 2018, p. 14.
evaluation has been prepared to consider all of the business issues, costs, benefits and risks and assess options such as employing more in-house staff to reduce some of the risks and management costs arising from the current extent of contracting of this critical and sensitive national security function.

2.46 In response, Defence advised that this work has not been undertaken and that ‘the business case that you’ve outlined is something that we haven’t done as a foundational first principles review.’

2.47 Defence did not provide the Committee with any evidence to demonstrate that it fully considered different service delivery models, including if it could utilise a smaller number of contractors, or if Defence could undertake a greater share of work itself. The Committee was unable to further explore these issues with a senior witness in a third public hearing as Defence was unavailable.

2.48 The Committee considers it would be good practice to fully and transparently assess various delivery options so Defence is able to demonstrate the optimal delivery arrangement, taking account of all of the associated costs and risks.

Recommendation 5

2.49 The Committee recommends that the Department of Defence prepare a full business case to consider the current and alternative service delivery models, taking account of projected future demand for vetting, the costs, benefits and risks of various approaches, and provide the findings of this to the Committee within 12 months.

Giving evidence

2.50 It is a key requirement of officials coming before the Joint Committee of Public Accounts and Audit to not only answer questions but to provide members of the Committee with the highest level of confidence that their concerns are being addressed.

2.51 It became clear at the Committee’s second public hearing that Defence was not able to provide the level of confidence or assurance the Committee required. An attempt was made to hold a third public hearing, however the Committee was advised that Defence witnesses were unavailable.

35 Mr Fortune, Department of Defence, Committee Hansard, Canberra, 17 August 2018, p. 2.
2.52 As a guiding principle, the Committee emphasises that departments should ensure all witnesses giving evidence before the JCPAA are adequately briefed on all matters relating to the Committee’s inquiry. In addition, departments should place careful consideration on the selection of witnesses to ensure they are in a position to answer the Committee’s questions in full.

2.53 Questions taken on notice during public hearings, and additional questions provided in writing, must be returned to the Committee in a timely fashion with careful and considered attention paid to the information provided.

2.54 As was the case for this inquiry, failure to provide the Committee with accurate and detailed answers to questions can necessitate the need for an additional public hearing and cause delays to the process of the inquiry.

2.55 The significant delays in receiving answers from Defence during this inquiry were unacceptable and could be considered disrespectful to the parliamentary committee process.

Review of evidence

Previous ANAO report

2.56 The ANAO previously reviewed the performance of AGSVA in ANAO Audit Report No.45 of 2014-15 Central Administration of Security Vetting, tabled in Parliament in June 2015. The ANAO concluded that the performance of centralised vetting had been mixed and expectations of improved efficiency and cost-effectiveness had not been realised. The ANAO found AGSVA had consistently failed to meet its clearance processing benchmark timeframes, had accumulated a backlog of over 13,000 clearances overdue for revalidation, and had inadequacies with its quality assurance processes, information systems and performance framework. The audit report recommended that Defence:

- implement a targeted audit program to assess Industry Vetting Panel contractors’ operations;
- introduce a program of internal peer review supplemented by periodic independent quality assurance of delegate decisions; and
- develop a clear pathway to achieve agreed timeframes for processing and revalidating security clearances.\(^{36}\)

In addition, the audit outlined a number of suggestions to improve the effectiveness of AGSVA’s operations, including that AGSVA:

- investigate the underlying causes of increasing numbers of clearance subjects cancelling clearances during the vetting process (which peaked at 34 per cent in 2015–16);
- strengthen its controls for managing sensitive personal information captured as part of the vetting process (including details of personnel medical and criminal records);
- improve the quality of its performance measurement and reporting; and
- consider how best to provide feedback to client entities on security concerns identified during vetting, to facilitate those entities’ monitoring of affected personnel.\(^{37}\)

**Clearance rates**

The Audit Report stated that timeframes for positive vetting clearances had deteriorated significantly since the previous audit. However, for other security levels, the percentage of cases completed within benchmark timeframes had improved.\(^{38}\)

The positive vetting clearance backlog was discussed extensively during the public hearing for the inquiry. The Defence representative, Mr Daniel Fortune, explained how the backlog was being dealt with:

>We commenced the remediation program in 2016. It is achieving really good results. We’ve cleared the initial backlog for new cases, which was 1,200 about this time last year. That is now down to 50 or in the dozens. We’ve increased capacity to meet current demand and planned future demand. While the time frames for new clearances are still higher than we’d like, we’re on a trajectory to return to our benchmark time frame by June of next year.\(^{39}\)

Mr Fortune also provided some performance figures on clearances:

>We’ve increased completions in the last three years by 250 per cent. That’s from 701 at the end of 2014-15, which was the backlog crisis point. We completed over 2,450 completions in the last financial year.\(^{40}\)


\(^{39}\) Mr Daniel Fortune, Assistant Secretary Vetting, Department of Defence, *Committee Hansard*, Canberra, 17 August 2018, p. 2.

\(^{40}\) Mr Fortune, Department of Defence, *Committee Hansard*, Canberra, 17 August 2018, p. 2.
2.61 However, during that period, the backlog grew as demand remained.\textsuperscript{41}

2.62 Mr Fortune provided details on the priorities for completing clearances:

\ldots we’re focused on new clearances—we call them ‘initials’ and ‘upgrades’—so we can get people into the workforce. Our priority there has been to support capabilities for the national intelligence community, particularly the Signals Directorate’s transformation into a statutory agency. So it’s a really positive story and the backlog for initial clearances has been removed.\textsuperscript{42}

2.63 In response to Committee questioning, Mr Fortune discussed upscaling of resources and responsiveness in meeting anticipated demands:

We’ve increased our internal capacity of vetting officers to grow capacity, and, importantly, we’ve increased our engagement with industry. Industry do about 85 per cent of all of our clearances and an increasing number of the positive vetting. As an example, two years ago they did 150 clearances; at the end of this financial year just finished, they did over 1,600\ldots We’re also doing business reform to drive those time frames down. We completed over 3,000 recommendations in the last financial year. We’ve increased our understanding of what the demand looks like. We work closely with the intelligence agencies and our colleagues across government to understand what they’re demanding\ldots So we’re confident that—as I outlined—our capacity now meets planned and increased demand. Our focus is to do them faster, and to continue to calibrate demand and our capacity as required.\textsuperscript{43}

2.64 During the public inquiry questions were raised regarding the costs, benefits and risks arising as a result of the outsourcing that has now occurred. Committee members were interested to understand if a cost-benefit evaluation has been prepared where all of the business issues and costs and benefits of employing more in-house staff and reducing some of the risks of contracting out to industry partners.

2.65 In response, Mr Fortune advised that this work had not been undertaken and that ‘the business case that you’ve outlined is something that we haven’t done as a foundational first principles review.’\textsuperscript{44}

\textbf{ICT and documentation issues}

\begin{flushright}
\textsuperscript{41}Mr Fortune, Department of Defence, Committee Hansard, Canberra, 17 August 2018, p. 2.
\end{flushright}

\begin{flushright}
\textsuperscript{42}Mr Fortune, Department of Defence, Committee Hansard, Canberra, 17 August 2018, p. 2.
\end{flushright}

\begin{flushright}
\textsuperscript{43}Mr Fortune, Department of Defence, Committee Hansard, Canberra, 17 August 2018, pp. 2-3.
\end{flushright}

\begin{flushright}
\textsuperscript{44}Mr Fortune, Department of Defence, Committee Hansard, Canberra, 17 August 2018, p. 15.
\end{flushright}
The current case management system

2.66 AGSVA’s current case management system, PSAMS2, supports vetting officers to manage clearances by providing workflow guidance. The system automatically generates tasks for completion by AGSVA vetting officers and delegates. Those tasks may include reviewing a file, undertaking an external check, or making an assessment decision.\(^\text{45}\)

2.67 However, PSAMS2 does not enforce completion of all tasks, even when such tasks are required to issue a clearance. For example, during the audit, the ANAO identified three recent cases relating to PV clearances that had progressed to a vetting decision without an ASIO check being completed.\(^\text{46}\)

2.68 Due to concerns about system stability, AGSVA has not been able to provide its vetting services contractors with access to PSAMS2. This results in clearance records being communicated via both mail and email, with contractors accumulating a substantial volume of hard-copy and electronic information. Potentially sensitive information is communicated outside of Defence’s secure ICT environment.\(^\text{47}\)

2.69 The existing system also suffers from substantial data quality issues. The Audit Report identified errors and discrepancies in biographical data of clearance holders. For example, there were clearance holders over the age of 100, under the age of 10 and a small number with a birthdate in the future. There were also many cases of primary clearances with revalidation dates more than five years in the past. The ANAO suggested that AGSVA take a more proactive approach to identifying, preventing and resolving anomalous data.\(^\text{48}\)

2.70 Defence acknowledge that the current systems is inadequate and noted that improvements should be evident from late 2020 with an ICT transformation project scheduled for full operational capacity in 2023: At the public hearing for the inquiry, the Defence representative, Mr Fortune, discussed the development of a new case management system and the timeframe for its establishment:

> Clearly, [PSAMS 2] is not fit for purpose, and Defence has a significant investment in the new ICT transformation project, which will become capable,


initially, in 2020. So in the time from 2023, with full operational capability, it
talks about some really sophisticated continuous assessment. But in terms of
the case management and the foundational system being more secure, more
digitised and more automated, the plan is to deliver that capability in late
2020.\textsuperscript{49}

\textbf{Handling of documentation}

2.71 During the public hearings for the inquiry, the Committee questioned
Defence extensively regarding the safe handling of sensitive and classified
documentation.

2.72 Currently, vetting contractors cannot interact with the existing case
management system. Information is largely transferred in paper form:

\ldots primarily, the e-pack that we receive through the Defence environment is
managed through hard copy printing and then safe-handed couriered to the
industry providers once it’s printed out. It’s largely a paper based system,
managing what we call the ‘protective security’ file, or the ‘personal security’
file, where the sensitive data is held in hard copy. There is email exchange, but
the information is classified ‘sensitive: personal’; it’s not classified in a security
sense. Therefore, in relation to the cyber risks around that, as I said, it’s best
practice—we audit that, we look to support whitelisting and how those ICT
systems and email connectivities are managed.\textsuperscript{50}

2.73 When asked by the Committee about the transfer of ‘hard copy’ files,
Defence stated that ‘AGSVA uses the national Defence contract for courier
services, including classified ‘safe hand’\textsuperscript{.51} At the time of the second public
hearing currently only TOLL Group,’ a member of the Defence Industry
Security Program (DISP) was used by AGSVA and the IVP companies to
transfer files.\textsuperscript{52} Defence told the Committee that ‘AGSVA has a strict security
protocol for movement of personal security files by TOLL, which includes
double-sealed packaging inside tamper-evident containers’.\textsuperscript{53}

2.74 When asked what happens in the event of a misaddress, Defence stated:

AGSVA has identified only one example of a consignment of Personnel
Security Files misaddressed to an Industry Vetting Panel (IVP) company in the

\textsuperscript{49} Mr Fortune, Department of Defence, \textit{Committee Hansard}, Canberra, 17 August 2018, p. 4.
\textsuperscript{50} Mr Fortune, Department of Defence, \textit{Committee Hansard}, Canberra, 17 August 2018, p. 4.
\textsuperscript{51} Department of Defence, \textit{submission 6.2}, p. 6.
\textsuperscript{52} Department of Defence, \textit{submission 6.2}, p. 2.
\textsuperscript{53} Department of Defence, \textit{submission 6.2}, p. 6.
past five years. This was not a positive vetting case. In this instance, the Defence approved courier, Toll, was unable to deliver the consignment to an industry vetting company as it had been misaddressed to one of the company’s regional offices. It is a requirement of AGSVA that consignments are signed for. As there was no one present to sign for the consignment, Toll returned the consignment to AGSVA the following day.

The consignment was then readdressed to the IVP company’s correct regional office and successfully delivered the following day.  

2.75 The Committee asked Defence to provide further information on the management of risks associated with the transfer of sensitive information via commercial courier services. Mr Fortune explained:

We understand there are challenges in managing the information exchange. That’s why there is significant investment in the new platform that we are working to deliver. In the meantime we are working with the arrangements that we are overseeing and assuring to deliver the capabilities that we need to drive the time frames down and to generate the clearances required for the workforce … We’ve got a system of oversight to ensure that the risks are managed and to satisfy ourselves through a program of audits that our partners are aware of those risks and manage their ICT. We advise them and support them in achieving their compliance.

2.76 When asked if contracted vetting service providers were currently compliant with the Essential Eight (a list of mitigation strategies to assist organisations in protecting their systems against a range of cyber threats), the Defence response to the question taken on notice stated that compliance is not mandatory. However, Defence explained that achievement of non-mandatory elements of the Essential Eight is managed through an ongoing process of information, communication and technology review and audit.

2.77 Defence further discussed its external review and auditing program:

Defence requires that all companies handling sensitive or classified information be members of the Defence Industry Security Program (DISP) and meet all Defence security requirements. All members of the Industry Vetting

54 Department of Defence, submission 6.2, p. 6.

55 Mr Fortune, Department of Defence, Committee Hansard, Canberra, 17 August 2018, p. 4.


57 Department of Defence, submission 6.2, p. 6.
Panel (IVP) are members of the DISP. Information provided to the IVP providers is handled in accordance with Defence security requirements, which includes mandatory information, communication and technology controls. The 14 IVP companies currently assigned to complete positive vetting cases are accredited against the Australian Signals Directorate Top Four cyber security requirements. This is a mandatory compliance under the DISP.\textsuperscript{58}

**Foreign ownership and contractor assurance**

2.78 The Committee pursued information on the Industry Vetting Panel (IVP) companies that currently conduct vetting for government agencies, seeking assurance that those entities do not have international ownership or work for other countries.

2.79 Defence told the Committee that all IVP companies are required to be members of the Defence Industry Security Program (DISP) in which each company must pass a Foreign Ownership, Control and Influence (FOCI) assessment prior to receiving their accreditation.\textsuperscript{59} Defence explained:

> Defence requires companies applying for DISP membership to provide a detailed declaration outlining their foreign engagement. This includes: holdings by foreign people, corporations or governments; key position holders’ links to foreign people or countries; contracts or other arrangements with foreign people or countries; revenue streams from foreign people, corporations or countries; and any other foreign control or influence indicators. A FOCI assessment then reviews the company’s FOCI declaration against an international FOCI standard, set by the Multi-National Industrial Security Working Group (MISWG).\textsuperscript{60}

2.80 Defence noted that ‘in undertaking FOCI assessments, a range of open source, commercial and intelligence sources may be reviewed to verify FOCI information supplied and to assess risks’.\textsuperscript{61}

2.81 Defence also explained that further security assurance is provided by AGSVA’s contractual arrangements (Deed of Agreement) with vetting companies:

> … which specifies that no classified information or official material furnished or generated under the Deed of Agreement can be disclosed to any third party.

\textsuperscript{58} Department of Defence, *submission 6.1*, p. 2.

\textsuperscript{59} Department of Defence, *submission 6.3*, p. 5.

\textsuperscript{60} Department of Defence, *submission 6.3*, p. 5.

\textsuperscript{61} Department of Defence, *submission 6.3*, p. 5.
Under the Deed of Agreement, companies must comply with all relevant Defence policy, including Defence security policy and declaring any actual, potential and perceived conflict of interest. No company has advised of any conflict of interest.  

2.82 The Department of Defence also confirmed that at the point of the February public hearing, ‘one company providing positive vetting services for Defence has one UK-national, Australian resident Director’, and that ‘no other companies providing positive vetting services list foreign directors’.  

2.83 The Committee questioned Defence on the impact of the change in management to AIM Screening, one of its current contractors.  

2.84 Defence explained that AIM Screening (trading as RISQ Group) does not provide positive vetting services for Defence, but was an IVP, and current member of the DISP. At the time of the February public hearing, Defence noted that AIM Screening was up to date with its FOCI reporting obligations under the DISP.  

2.85 When questioned about the ability of the 14 IVP companies to conduct work for foreign governments, Defence told the Committee that it was unable to prevent IVP companies or their personnel from undertaking work for foreign governments ‘as there is no specific restraint of trade restriction under the Conditions of the Deed of Standing Offer’. Defence noted that the Deed did include strict security requirements for an IVP company to comply with Defence’s ‘security policies and processes, including maintaining membership of the DISP and complying with the Defence Security Principles Framework.’  

2.86 The Committee questioned Defence as to the clearance requirements of vetting staff employed by the companies that currently conduct vetting for government agencies. Defence responded:  

The FOCI assessment considers the company, Directors/officers, and key personnel. Industry Vetting Panel staff who are designated as specified personnel (this includes vetting officers as well as any non vetting staff that
handle or access any official material) are required to hold an Australian Government security clearance.

DISP members, as part of ongoing reporting requirements, must update their FOCI information whenever there are any changes to their FOCI status.\textsuperscript{67}

2.87 Defence further confirmed that all industry vetting officers working on positive vetting (PV) clearances are Australian citizens, and stated that ‘there are no officers working under a waiver’.\textsuperscript{68}

**Retention of sensitive or classified information**

2.88 The Committee was concerned that sensitive or classified material, or indeed any identifying information, remained with a security vetting contractor, in hard copy or in digital form, after the completion of the vetting process.

2.89 Defence stated that security-related information provided to IVP companies is handled in accordance with defence industry security requirements. Defence further explained:

> IVP companies ensure all documentation relating to a clearance process is attached to the appropriate Personal Security File (PSF) and returned to AGSVA when a case is completed. When the PSF is returned to AGSVA, companies immediately destroy any hard copy duplicates of information that was included in the PSF.\textsuperscript{69}

2.90 Defence also explained that electronic documentation can be kept on an ICT certified system for up to 90 days after the PSF is returned to AGSVA, which allows AGSVA to obtain further or missing documentation, if required, during the decision making stages.\textsuperscript{70}

2.91 However, during the public hearings, Defence noted that ‘disaggregated’ information is retained on contractors’ systems beyond 90 days. The example given was of a record of the fact that there had been an interview conducted and a named referee contacted.\textsuperscript{71}

2.92 While Defence told the Committee that it had written to the required IVP companies to reinforce the requirement to delete all information after 90

\textsuperscript{67} Department of Defence, *submission 6.1*, p. 7.

\textsuperscript{68} Department of Defence, *submission 6.3*, p. 10.

\textsuperscript{69} Department of Defence, *submission 6.1*, p. 4.

\textsuperscript{70} Department of Defence, *submission 6.1*, p. 5.

\textsuperscript{71} Mr Fortune, Department of Defence, *Committee Hansard*, Canberra, 12 February 2019, p. 11.
days, the Committee was not able to ascertain from Defence what process
are in place to ensure the requirement is currently being met.72

2.93 Defence noted that ‘all 14 IVP companies currently assigned to complete
positive vetting cases are accredited against the Australian Signals
Directorate (ASD) Top 4’, which is ‘a mandatory compliance under the
DISP’. However, Defence advised the Committee that compliance with the
ASD Essential Eight is not mandatory.73

2.94 Defence confirmed to the Committee that all 14 IVP companies currently
assigned to complete positive vetting cases are compliant with the
Information Security manual and the DISP Top 4 for cybersecurity.74

2.95 Defence stated that IVP companies are subject to random checks of ICT
storage systems as part of AGSVA audit processes and performance review
meetings.75

2.96 The Committee questioned Defence on who was responsible for conducting
the audits and how they are verified, but was unable to ascertain a clear
answer from Defence. Defence gave the Committee assurances that the
companies were reporting that they are cyber resilient, but was unable to
explain what compliance mechanisms were in place to verify the reporting is
accurate and meets the mandated standards.76

72 Mr Fortune, Department of Defence, Committee Hansard, Canberra, 12 February 2019, p. 12.
73 Mr Fortune, Department of Defence, Committee Hansard, Canberra, 12 February 2019, p. 8.
74 Mr Fortune, Department of Defence, Committee Hansard, Canberra, 12 February 2019, p. 8.
75 Department of Defence, submission 6.1, p. 5.
76 Mr Fortune, Department of Defence, Committee Hansard, Canberra, 12 February 2019, p. 9.
3. Domestic Passenger Screening - Follow-Up

3.1 This chapter sets out the Committee’s findings in relation to the Department of Home Affairs’ implementation of recommendations from Australian National Audit Office (ANAO) Report No. 43 (2017-18), Domestic Passenger Screening – Follow-Up. It comprises the following sections:

- Committee conclusions and recommendations
- Review of evidence

Committee conclusions and recommendations

3.2 The Department of Home Affairs (the department) undertakes domestic passenger screening in order to prevent prohibited items such as weapons and explosives from being carried onto aircrafts. The detection and control of prohibited items requires the use of specialised equipment and screening personnel at 62 security controlled airports across Australia. Passenger screening needs to be conducted efficiently and must meet legislated and regulatory requirements.¹

3.3 The ANAO tabled Auditor-General Report No. 5 (2016-17), Passenger Security Screening at Domestic Airports on 31 August 2016. This performance audit made five recommendations aimed at improving the department’s (then, the Department of Infrastructure and Regional Development) regulatory performance. The audit found that the department:

---

...was unable to provide assurance that passenger screening was effective, or to what extent screening authorities had complied with the Regulations, due to poor data and inadequate records. The ANAO also found that the Department did not have meaningful passenger screening performance targets or enforcement strategies and did not direct resources to areas with a higher risk of non-compliance.\(^2\)

3.4 The ANAO undertook a follow-up performance audit in 2017-18 due to the significance of the findings and recommendations of the previous audit, and the response from the department ‘advising that a number of initiatives to address the shortcomings identified were already underway’.\(^3\) The follow-up audit was tabled on 29 May 2018 and focused on the extent to which the Department of Home Affairs (the Office of Transport and Security was moved into the Department of Home Affairs on 20 December 2017), had implemented the five recommendations from the previous report. The follow-up audit examined the department’s compliance monitoring program, learning and development framework, and performance monitoring and reporting arrangements.\(^4\)

3.5 The follow-up audit found that as at March 2018, the department had implemented one and partially implemented four of the five recommendations from the previous audit.\(^5\) In its response to the follow-up audit findings, the department noted that it had made progress despite the audit being initiated less than 12 months after the previous audit and the department responding to a significant aviation security event in July 2017.\(^6\)

3.6 The follow-up audit made three recommendations and concluded that although the department had made progress, it was not yet ‘well placed to provide assurance that passenger screening is effective and that screening authorities comply with the Regulations’.\(^7\) The department agreed with all three recommendations in the follow-up audit, but disagreed with the ANAO’s conclusion:

\(^6\) ANAO Report No. 43 (2017-18), p. 40; Mr Angus Kirkwood, Acting First Assistant Secretary, Aviation & Maritime Security Division, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 4.
\(^7\) ANAO Report No. 43 (2017-18), p. 8.
I do not agree with comments made in the report about the Department’s inability to provide assurance that screening authorities comply with the regulations. As acknowledged in the report, the Department measures the compliance of screening authorities with the regulations on a regular basis and these activities assure us that the authorities are compliant. Where they are not, further compliance action is taken.8

3.7 At the public hearing, the department further explained that it had a comprehensive compliance regime and that the ‘issues identified by the ANAO are but one narrow slice of performance measures that could be looked at’.9 The department stated that the ‘way that the audit focused that finding was very narrow on the type of measures they were looking at. It doesn’t take into account the full spectrum of our compliance program’.10

3.8 The ANAO responded that the follow-up audit focused on the department’s progress in implementing the five recommendations from the previous audit. As four of the recommendations were not implemented, the ANAO could not conclude that the department was ‘now well placed to be able to provide that evidence or information about their performance’.11

3.9 The Committee agrees that follow-up audits are important for holding entities to account and examining whether entities respond appropriately to audit findings and agreed recommendations.12 The Committee notes that the prevention of prohibited weapons and explosives from being carried onto aircraft is a matter of public interest and safety, and is concerned that the ANAO’s follow-up audit concluded that the department is still ‘not yet well placed to provide assurance that passenger screening is effective and that screening authorities comply with the Regulations’.13

Recommendation 6

3.10 The Committee recommends that the Australian National Audit Office consider conducting a follow-up audit in 2019-20, focusing on the

---

9 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 1.
10 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 1.
12 Australian National Audit Office (ANAO), Submission 7.1, p. 1.
department’s implementation of eight agreed ANAO recommendations and considering the department’s entire compliance program.

3.11 The Committee is concerned that both the previous audit and the follow-up audit identified issues regarding the quality of data used by the department. The department has acknowledged that ‘the ease of use of the system is not perfect’ and that in response to challenges with data, it has developed ‘arrangements to effectively work around some of those challenges’.  

3.12 The Committee notes that the department has commenced producing two main analytical products to inform compliance activities and will undertake an upgrade of the Regulatory Management System (RMS) in the first quarter of 2019. The follow-up audit outlined that the department has made improvements to the quality and reliability of data in the RMS, however issues still remained: inconsistent and incomplete data, and constraints on data extraction and reporting. The department obtained approval to develop a data product suite in November 2017 to address issues regarding analysis and reporting across systems, however the ANAO reported that as at March 2018, the department had not developed an associated plan.

3.13 The Committee considers that the use of baseline data – data which measures conditions before a project or initiative is commenced for the purposes of later comparisons – is important in measuring the outcomes of projects and initiatives. Following the findings of both audit reports, the Committee expects that the department will prioritise improvements to data quality, and measure and report on the improvements.

Recommendation 7

3.14 The Committee recommends that the Department of Home Affairs:

- gather an appropriate baseline data set prior to the implementation of Regulatory Management System upgrade in the first quarter of 2019;

- monitor and review the outcomes of the upgrade against the baseline data set, particularly whether data quality is improving; and

- either prioritise an additional upgrade to the Regulatory Management System in order to establish an efficient and effective reporting

14 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 1.

function, or prioritise the development of the data product suite (as was approved on 10 November 2017) in order to address the limitations to data quality and performance reporting identified in the ANAO report.

3.15 The Committee is concerned that the department has not provided detailed information regarding milestones and timeframes for the implementation of the compliance and enforcement framework. Further, the department has stated that the three-year timeframe may be impacted by 12 to 24 months if the department decides to proceed with the development of a centralised case management system.\textsuperscript{16} Considering the importance of compliance and enforcement in providing assurance that passenger screening is effective, the Committee recommends the department provide more information regarding the implementation of the compliance and enforcement framework.

**Recommendation 8**

3.16 The Committee recommends that the Department of Home Affairs report back to the Committee on progress in the implementation of the compliance and enforcement framework in detail, including objectives, timeframes, milestones, lines of responsibility, performance measures, evaluation and reporting arrangements, and further information on the centralised case management system.

3.17 The Committee notes that the department has commenced delivery of a learning and development program which involves staff undertaking qualifications in a Certificate IV in Government and a Diploma of Government. The department has outlined that staff will undertake training for core capabilities, specialist capabilities, and system test training.\textsuperscript{17} However, the Committee is concerned that the information provided by the department does not wholly address whether staff will receive training in the use of the Regulatory Management System to improve data quality, as was the original intention of Recommendation No. 4 of ANAO Report No. 5 (2016-17).


\textsuperscript{17} Department of Home Affairs, *Submission 8.1*, pp. 2-3; Mr Kirkwood, Department of Home Affairs, *Committee Hansard*, Canberra, 19 September 2018, p. 4.
Recommendation 9

3.18 The Committee recommends that the Department of Home Affairs report back to the Committee on training undertaken by staff in relation to the Regulatory Management System, and whether improvements to data quality, reliability and accuracy are being measured and achieved.

3.19 The Committee notes that the department commenced delivering training as part of the learning and development program in February 2018, all staff will be qualified by the start of 2019, and an annual re-accreditation process will be undertaken by all staff.18 At the public hearing, the department stated that it was satisfied that available baseline data will enable monitoring and evaluation of the effectiveness of the training.19

3.20 The Auditor-General explained that the previous audit identified that the department had not monitored and collected data on staff attendance at training.20 Further, the Auditor-General had previously suggested that the department use the training needs analysis completed in 2017 as baseline data for the purposes of monitoring and evaluating the learning and development framework.21

3.21 The Committee is concerned that while the department has established and made available data points for the monitoring and evaluation strategy, the data by itself is not enough to address concerns or identify emerging risks without adequate monitoring and evaluation activities.

3.22 The Committee considers that the department has the opportunity to strengthen the available baseline data for the purposes of measuring the effectiveness of the learning and development framework.

Recommendation 10

3.23 The Committee recommends that in relation to the learning and development framework, the Department of Home Affairs:

---

18 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 4; Department of Home Affairs, Submission 8.1, p. 1.
19 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 6.
20 Mr Grant Hehir, Auditor-General, ANAO, Committee Hansard, Canberra, 19 September 2018, p. 6.
 establish a formal monitoring mechanism to provide assurance that all ongoing and new operational staff have undertaken the required qualifications and re-accreditation; and

 consider using the results of the training needs analysis from February 2017 as baseline data in the monitoring and evaluation of the learning and development framework.

3.24 The Committee notes the long-term delays in the department’s implementation of performance measures for passenger screening.22 The Committee also notes that the ANAO reported that full implementation was expected by February 2019,23 however the department later advised that there was no expected implementation date.24 The Committee is concerned that there is no longer a set implementation date and agrees that in order to achieve the expected benefits, implementation of accepted recommendations should be timely and in line with the intended outcomes.25

Recommendation 11

3.25 The Committee recommends that the Department of Home Affairs report back to the Committee on the implementation of performance measures for passenger screening, including:

 the outcomes of the trial implementation period of performance measures with industry participants; and

 the department’s target date for full implementation of performance measures.

Review of evidence

3.26 This section reviews the evidence received by the Committee regarding the department’s compliance monitoring, learning and development, and performance monitoring and reporting.


23 ANAO Report No. 43 (2017-18), p. 34.

24 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, pp. 6-7.

Compliance monitoring

Data analysis function

3.27 The previous audit found that the department ‘had limited information about the compliance history of individual industry participants and lacked reliable data and analysis to identify systemic issues, or compare performance across industry participants’. The ANAO recommended that the department establish a data analysis function to capture accurate and reliable compliance data in order to identify trends in non-compliance.

3.28 The department consequently established a data analysis function that delivered a single analysis of compliance information in July 2017. The analysis provided a ‘breakdown of compliance activities conducted for each category of airport and aircraft operator, the number of findings by type for each state, and the number of findings per security mitigation category’.

3.29 The ANAO found that the July 2017 analysis ‘did not identify trends in non-compliance or identify industry participants that required a higher level of support to comply with the regulated requirements’. The follow-up audit recommended that in implementing Recommendation No.2 from the previous audit:

The Department should ensure that its approach delivers a meaningful analysis of passenger screening compliance activities and outcomes. The analysis should: be capable of accurately identifying non-compliance trends; generate results that are used to inform the development of the risk and compliance prioritisation ratings; and be incorporated into subsequent compliance monitoring programs.

3.30 The ANAO also noted concerns regarding compliance data quality; the ANAO examined the compliance data extracted from the Regulatory Management System (RMS) and found that inconsistent and incomplete data was still being entered into the system. Further, the retrieval of data from the RMS was limited for the purposes of analysis and reporting due to

---

the use of free text fields, ‘which do not facilitate easy retrieval for reporting and analysis’. 31

3.31 On 10 November 2017, the department obtained approval to develop a data product suite in order to address issues within the current systems, including:

- the number of disparate business systems used to store data;
- the quality and continuity of data sets;
- limited data extraction and reporting capabilities; and
- different data structures and definitions used across the various business systems in use. 32

3.32 As at March 2018, the department had not yet progressed with a plan outlining how to develop the data product suite, improve the systems’ ability to provide meaningful analysis of compliance activity and outcomes, and enable comprehensive reporting. 33

3.33 At the public hearing, the department noted that the RMS system remains in use; however the department is planning an upgrade of the RMS in the first quarter of 2019. The upgrade will focus on simplifying the data entry and improving data quality by completely revising the user interface. 34

National Compliance Plan

3.34 The previous audit found that the department ‘was unable to assess the risks of non-compliance or identify systemic non-compliance and apply resources where the risk is higher’, due to ineffective processes in collecting, storing and retrieving data for the purposes of evaluating individual industry participant performance. 35 The ANAO recommended that in order for the department to focus compliance resourcing on areas with a higher risk of non-compliance, the outcomes of compliance activities should be incorporated into future compliance plans. 36

33 ANAO Report No. 43 (2017-18), pp. 21-22.
34 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 5.
3.35 The single analysis delivered in July 2017 was not used in the development of the National Compliance Plan (NCP) for 2017-18. The department instead developed the NCP by extracting other compliance data from the RMS and Microsoft Excel regional office work plans. The ANAO concluded that as a result, the NCP was not informed by ‘an analysis of trends in non-compliance or identify industry participants exposed to a higher risk of non-compliance’.37

3.36 In response to the follow-up audit recommendation, the department stated:

The Department has established a dedicated team responsible for producing analytical products that inform compliance activities. Analysis is informing both the annual National Compliance Plan (NCP) and the targeting of industry participants to ensure that compliance activities are directed to the highest risks. The NCP is updated, and program delivery adjusted, based on a monthly review of compliance activity results, non-compliance trends, and threat and risk information.38

3.37 At the public hearing, the department further outlined that ‘we are now in the position, following the follow-up audit, to implement the type of analytical products that feed into the national compliance program which were recommended by the ANAO’.39 The department explained that two main analytical products are informing the NCP in 2018-19: one product is the analysis of covert system test results which aims to identify systemic issues, such as at particular screening points or access points at airports. The department confirmed that this is an increasing program of approximately 1000 covert system tests to be conducted over 2018-19.40

3.38 The follow-up audit outlined that the department ‘directs compliance resources to categories of airports and airline operators that present a higher security risk’.41 The department determines the risk and compliance prioritisation ratings of categories of airline operators and airports, and resources and compliance activities are directed based on these ratings. However, the department does not identify individual industry participants – individual airports and airline operators – where the risk of

38 Department of Home Affairs, Submission 8, p. 1.
39 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 2.
40 Mr Richard Farmer, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 3.
non-compliance is higher, and does not direct compliance resources accordingly.\textsuperscript{42}

3.39 At the public hearing, the department outlined that the other main analytical product that informed the NCP in 2018-19 was the analysis of industry participant compliance history. This analysis examines individual industry participants and trends in their compliance history, assessing whether compliance is improving or deteriorating.\textsuperscript{43}

\textit{Compliance and enforcement framework}

3.40 The previous audit found that the department ‘did not have an enforcement policy and did not utilise the full suite of enforcement actions available to it’.\textsuperscript{44} Consequently, the previous audit suggested the department develop a clear enforcement strategy.\textsuperscript{45}

3.41 Following the previous audit, the department provided training to all transport security inspectors to improve consistency in the issuing of non-compliance notices and observations. The department also began to ‘make greater use of additional enforcement options such as infringement notices’.\textsuperscript{46}

3.42 The follow-up audit found that the department developed a strategic plan for 2017-20, a compliance and enforcement framework, and an implementation plan.\textsuperscript{47} The strategic plan broadly outlines the department’s compliance approach and indicates that the department ‘intends to build its capacity to undertake enforcement action over the course of the next three years’.\textsuperscript{48}

3.43 The ANAO outlined that the implementation plan included components such as the management of enforcement activities, the proposed delivery model, the establishment of an enforcement team, and suggested training for personnel focused on enforcement and investigative skills. The

\begin{itemize}
\item \textsuperscript{42} ANAO Report No. 43 (2017-18), p. 23.
\item \textsuperscript{43} Mr Farmer, Department of Home Affairs, \textit{Committee Hansard}, Canberra, 19 September 2018, p. 3.
\item \textsuperscript{44} ANAO Report No. 43 (2017-18), p. 26.
\item \textsuperscript{45} ANAO Report No. 43 (2017-18), p. 26. The previous audit, ANAO Report No. 5 (2016-17), provided this suggestion in paragraph 3.18.
\item \textsuperscript{46} ANAO Report No. 43 (2017-18), p. 27.
\item \textsuperscript{47} ANAO Report No. 43 (2017-18), pp. 26-27.
\end{itemize}
implementation plan also identified that the department should provide clear guidance indicating the various enforcement options and the escalation process to assist in the management of non-compliance. At the time of the follow-up audit, the implementation plan was not yet approved.\textsuperscript{49}

3.44 At the public hearing, the department indicated that the three-year timeframe for the implementation of the compliance and enforcement framework included an initial focus on the learning and development framework. This was to ensure that personnel are capable of ‘effective decision-making, to collect evidence effectively and to have consistency and lawful decision-making by our inspectors’\textsuperscript{50}. Training for staff commenced in February 2018 and included staff enforcement capability training.\textsuperscript{51}

3.45 The department argued that the absence of a finalised implementation plan does not mean ‘that we aren’t doing very effective and strong compliance already. We are very active in this space’.\textsuperscript{52}

3.46 The department further explained that the implementation plan outlined ‘that the core elements of the enforcement capability will be implemented within 12 months’.\textsuperscript{53} The core elements include completing staff enforcement capability training and starting enforcement trials, and developing enforcement procedures and supporting materials. In December 2017, the department also commenced a limited infringement notice trial which has now been expanded nationally. The department explained that ‘the trial enables application of staff enforcement training, with outcomes informing the development of enforcement procedures’.\textsuperscript{54}

3.47 However, the timeframe for the implementation of the framework may be extended by 12 to 24 months if the department decides to develop a centralised case management system.\textsuperscript{55}

Learning and development

\textsuperscript{49} ANAO Report No. 43 (2017-18), pp. 26-27.

\textsuperscript{50} Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 2.

\textsuperscript{51} Department of Home Affairs, Submission 8.1, p. 1.

\textsuperscript{52} Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 3.

\textsuperscript{53} Department of Home Affairs, Submission 8.1, p. 1.

\textsuperscript{54} Department of Home Affairs, Submission 8.1, p. 1.

\textsuperscript{55} Department of Home Affairs, Submission 8.1, p. 1.
3.48 The previous audit found that departmental staff were not trained in using the Regulatory Management System (RMS), which resulted in significant issues with the completeness and accuracy of the data captured in the RMS. The ANAO recommended that the department ‘conduct a training needs analysis for users of the RMS system, deliver appropriate training and monitor its effectiveness’.56

3.49 The department initially advised that the training needs analysis would be completed by December 2016. However, the department decided to undertake a broader training needs analysis than the ANAO had recommended, and completed this analysis in February 2017. The department commenced consolidating the recommendations from the training needs analysis into a learning and development framework in June 2017. The department began delivering the training as per the learning and development framework in February 2018. Tailored specialist modules, including training on the RMS, were scheduled for delivery from June 2018.57

3.50 At the public hearing, the department explained that all operational staff had commenced ‘either a nationally recognised qualification in cert IV in government or a diploma in government’ in February 2018.58 This training includes core capabilities, specialist capabilities, and system test training, and all staff will complete the training program by November 2018 with assessments to take place throughout December 2018. IT system processes and ensuring the integrity of data entry are included in this training program.59

3.51 As part of the learning and development framework, all staff are required to complete training in core capabilities, and managers are required to complete leadership modules that include performance management, continuous improvement, and coaching and developing others. Staff will undertake re-accreditation and assessment on an annual basis. The core capabilities included in the training are:

- stakeholder engagement;
- communication and representation;
- principles of decision-making;

58 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 4.
59 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 4.
- administrative law and legislation;
- analysis and critical thinking; and
- judgement and evidence-based decision-making.\textsuperscript{60}

3.52 In addition to the core capabilities, there are two specialist capability streams which have been tailored to be role-specific to departmental staff, as outlined in Table 3.1.

\textsuperscript{60} Department of Home Affairs, Submission 8.1, p. 3.
Table 3.1  Role-specific capability streams for staff

<table>
<thead>
<tr>
<th>Regulatory assessment staff</th>
<th>Regulatory compliance staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment fundamentals</td>
<td>Compliance fundamentals</td>
</tr>
<tr>
<td>Preparing documentation and writing reports</td>
<td>Preparing documentation and writing reports</td>
</tr>
<tr>
<td>Continuous improvement</td>
<td>Continuous improvement</td>
</tr>
<tr>
<td>Analysis and judgement</td>
<td>Conducting audits and inspections</td>
</tr>
<tr>
<td></td>
<td>Acting on non-compliance</td>
</tr>
<tr>
<td></td>
<td>Foundation and advanced training courses for the covert system test function</td>
</tr>
</tbody>
</table>


3.53 The follow-up audit found that the department’s learning and development framework ‘broadly aligns with six of the seven principles for better practice in learning and development identified by the Australian Public Service Commission’. However, the learning and development framework did not include a monitoring and evaluation component. The ANAO found that the department was developing a monitoring and evaluation component, but as at March 2018 it was not yet finalised.

3.54 The monitoring and evaluation strategy was finalised in August 2018 and will commence from January 2019. These timeframes were agreed to allow for the implementation of the certificate IV qualification training program for operational staff in 2018. From January 2019, the department will ‘start monitoring those data points across our systems to see if we’re getting a lift in performance both in terms of data quality and in terms of outcomes’.

3.55 The department continuously examines the quality of the work being produced through the internal operations governance and quality assurance process within the division. This involves ongoing activities such as

---

63 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, pp. 4-5.
assessing whether appropriate procedures were followed, and undertaking the quality and assurance function within the division. The department explained that:

…setting January as the formal start point, that doesn’t mean that we’re not looking at the data now; it means in terms of technically doing the performance evaluation of the L&D framework, we’re starting the evaluation once the L&D implementation is complete.\textsuperscript{64}

3.56 At the public hearing, the Committee queried what baseline data the department was using to evaluate the performance of the delivery of the training. The department confirmed that it was satisfied that the baseline data that it had access to will enable it to monitor and evaluate the effectiveness of the training,\textsuperscript{65} and outlined:

…we’re looking at our internal audit process and quality assurance process. We’re looking at the actual data in our IT system, the regulatory management system itself, so we can see if we’re having quality control issues with the data and if that’s improving through time. We’re looking at our staff and development performance agreements and performance reviews, so those processes with staff, and also looking at training evaluation reports coming out of the L&D process.\textsuperscript{66}

3.57 Baseline data measures conditions before a project or initiative is commenced for the purposes of later comparisons. In response to the department’s explanation of the learning and development framework, the Auditor-General noted that the department’s implementation of a structured framework was a positive step. However, in terms of baseline data, the Auditor-General stated that:

I don’t think there would be much historic data to rely on, because there wasn’t any system for collecting that data or identifying who was trained or who wasn’t, according to the evidence that we saw in the previous audit.\textsuperscript{67}

3.58 The follow-up audit noted that in order to evaluate the extent to which the objectives of the framework are being met, the department may use the results of the training needs analysis as baseline data.\textsuperscript{68} The department’s

\textsuperscript{64} Mr Kirkwood, Department of Home Affairs, \textit{Committee Hansard}, Canberra, 19 September 2018, p. 5.
\textsuperscript{65} Mr Kirkwood, Department of Home Affairs, \textit{Committee Hansard}, Canberra, 19 September 2018, p. 6.
\textsuperscript{66} Mr Kirkwood, Department of Home Affairs, \textit{Committee Hansard}, Canberra, 19 September 2018, p. 5.
\textsuperscript{67} Mr Hehir, Auditor-General, ANAO, \textit{Committee Hansard}, Canberra, 19 September 2018, p. 6.
\textsuperscript{68} ANAO Report No. 43 (2017-18), p. 30.
response to the recommendation in the previous audit (Recommendation No.4), outlined that the training needs analysis would include an assessment of the skills, knowledge and capabilities of staff against their roles, which will be used to address gaps.69

Performance monitoring and reporting

Performance measures

3.59 The previous ANAO audit found that the department ‘did not have appropriate performance measures in place to determine whether passenger screening is effective’.70 As a result, the ANAO recommended that the department develop practical, achievable and measurable performance measures in consultation with stakeholders.71

3.60 Since 2002, four of 10 reviews conducted to investigate aviation security have specifically noted the need for the department to develop and implement performance measures. This includes ANAO Report No.26 (2002-03), Aviation Security in Australia. The department had commenced the process to develop performance measures on a few occasions since 2009.72

3.61 In October 2017, draft performance measures were approved by the department and circulated to industry stakeholders.73 The ANAO examined the performance measures developed by the department and found that that the performance data required was already being generated by most industry participants. Further, the reporting frequency and timeframes of the proposed measures were considered ‘practical and achievable from an industry perspective’.74

3.62 The follow-up ANAO audit explained that the department was due to commence the implementation of performance measures in March 2018 by initially undertaking a pilot program with a selection of industry participants. Wider implementation was to occur from 1 July 2018 as part of the department’s Enhanced Mandatory Reporting Project. The implementation of performance measures was to be finalised by February

70 ANAO Report No. 43 (2017-18), p. 32.
74 ANAO Report No. 43 (2017-18), p. 34.
As the department had developed but not yet implemented performance measures, the follow-up audit recommended that:

In implementing Recommendation No.3 from the previous audit, the Department should ensure that performance measures are established in a timely manner alongside an effective monitoring and review mechanism to provide assurance that the performance measures developed for passenger screening are practical, achievable and measurable.

3.63 At the public hearing, the department outlined that the trial period was underway – the pilot commenced in May 2018 and is due to be completed in October 2018. In response to the Committee query regarding when the department would achieve full implementation, the department responded:

We’ll have to assess the outcomes of the trial data with airports following the conclusion of the trial in October. Because we are relying on the provision of data from airport operators, we’ll have to agree with them on the timings that are practical in terms of settling the measures, and to establish a plan going forward from there.

3.64 When the Committee further queried if there was an expected implementation date, the department responded that:

I don’t think one has been set. We’re doing the trial to identify these issues, as we have said, and then we’ll have to take those into account in setting a reasonable path forward, given that we will be requiring industry to provide this information.

3.65 In response to the department’s explanation, the Auditor-General noted that the ANAO report outlined the original target implementation milestones for performance measures. The Auditor-General explained that the advice given by the department at the public hearing was different to the ANAO report and ‘seems to have a longer time frame associated with it’.

3.66 Following completion of the trial in October 2018, the department plans to undertake analysis of the results and commence further industry

75 ANAO Report No. 43 (2017-18), p. 34.
76 ANAO Report No. 43 (2017-18), p. 35.
77 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 6.
78 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 6.
79 Mr Kirkwood, Department of Home Affairs, Committee Hansard, Canberra, 19 September 2018, p. 7.
80 Mr Hehir, Auditor-General, ANAO, Committee Hansard, Canberra, 19 September 2018, p. 7.
consultation during the first quarter of 2019. Subject to regulatory approval, the department ‘will then develop regulatory amendments to require the mandatory provision of screening performance data’.\(^{81}\)

3.67 The department explained that the trial period for performance measures involves airports of varying sizes, system maturity, and data collection methods.\(^{82}\) The findings from the trial have highlighted that due to the range of industry participants and the variety in the systems used, ‘there are implementation issues with consistency of data and in individual airports’ ability to provide data in a consistent way’.\(^{83}\)

3.68 The department also outlined that this trial period was ‘an important aspect of testing that this data is in fact practical and achievable and measureable, as set out by the Audit Office’.\(^{84}\) The department is planning to assess whether the performance measures are practical, achievable and measurable, by considering:

- what data received through the trial provided valid measurement of passenger screening performance; and
- the industry’s ability to provide the Department with the data on a continual and consistent basis.\(^{85}\)

**Performance reporting**

3.69 The previous audit noted limitations to the department’s performance reporting, including the Regulatory Management System (RMS) not having a reporting function. The department initially addressed this issue by endorsing 15 operational reports; six of these reports were ‘high priority’ and would cost $160 000. Instead, the department chose to build the reporting function in-house.\(^{86}\)

3.70 The in-house reporting function involves the manual extraction of data from the RMS. As at December 2017, the RMS cannot produce ‘accurate standard reports such as industry participant contact details, and compliance histories

---

\(^{81}\) Department of Home Affairs, *Submission 8.1*, p. 4.

\(^{82}\) Mr Farmer, Department of Home Affairs, *Committee Hansard*, Canberra, 19 September 2018, p. 7.


\(^{84}\) Mr Kirkwood, Department of Home Affairs, *Committee Hansard*, Canberra, 19 September 2018, p. 6.

\(^{85}\) Department of Home Affairs, *Submission 8.1*, p. 4.

\(^{86}\) ANAO Report No. 43 (2017-18), p. 35.
of individual industry participants’. The follow-up audit concluded that the department has improved its capacity to provide reports to meet stakeholders’ business needs. However, the production of these reports is resource intensive due to the requirement to manually extract data from the RMS and Microsoft Excel based regional office work plans.

Senator Dean Smith
Chair

1 April 2019

87 ANAO Report No. 43 (2017-18), p. 35.
A. Terms of Reference and JCPAA Role

Terms of Reference

Any items, matters or circumstances connected with the following Auditor-General report:

- No. 38 (2017-18) Mitigating Insider Threats through Personnel Security
- No. 43 (2017-18) Domestic Passenger Screening - Follow-Up

Having considered Auditor-General Report 17-50 (2017-18) on 27 June 2018, the Joint Committee of Public Accounts and Audit resolved to conduct an inquiry based on the above Auditor-General reports.

Under section 8(1) of the legislation establishing the JCPAA, the Public Accounts and Audit Committee Act 1951, one of the duties of the Committee is to ‘examine all reports of the Auditor-General (including reports of the results of performance audits) that are tabled in each House of the Parliament’ and ‘report to both Houses of the Parliament, with any comment it thinks fit, on any items or matters in those … reports, or any circumstances connected with them, that the Committee thinks should be drawn to the attention of the Parliament’.

JCPAA Role

The purpose of the Joint Committee of Public Accounts and Audit (JCPAA) is to scrutinise the governance, performance and accountability of Commonwealth entities and companies—focusing on whether public money is used in an efficient, effective, economical and ethical manner. The JCPAA is therefore the Parliament’s joint public administration committee.
The Committee’s powers are contained within the *Public Accounts and Audit Committee Act 1951*.

The Committee examines all reports of the Auditor-General, adopting inquiries, including thematic inquiries, based on specific audit reports. In adopting inquiries based on audit reports, the Committee considers:

- the significance of the program or issues raised in audit reports
- the audited agencies response to the audit
- the potential public interest benefits in conducting an inquiry

The Committee examines a broad range of evidence. In addition to the ANAO reports, the Committee receives submissions from audited agencies and the public, and conducts public hearings. The Committee also considers relevant public sector frameworks and findings of other relevant reviews, reports and audits. In particular, the Committee references the relevant sections of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), PGPA Rule 2014, and associated resource management guidance. As the primary piece of Commonwealth resource management legislation, the PGPA Act establishes a single system of governance and accountability for public resources.
B. ANAO Conclusions and Recommendations


Conclusion (p.8)

The effectiveness of the Australian Government’s personnel security arrangements for mitigating insider threats is reduced by: AGSVA not implementing the Government’s policy direction to share information with client entities on identified personnel security risks; and all audited entities, including AGSVA, not complying with certain mandatory PSPF controls.

AGSVA’s security vetting services do not effectively mitigate the Government’s exposure to insider threats. AGSVA collects and analyses information regarding personnel security risks, but does not communicate risk information to entities outside the Department of Defence or use clearance maintenance requirements to minimise risk. Since the previous ANAO audit, AGSVA’s average timeframe for completing Positive Vetting (PV) clearances has increased significantly. AGSVA has a program in place to remediate its PV timeframes, and it has established a comprehensive internal quality framework. AGSVA plans to realise many process improvements through procuring a new information and communications technology (ICT) system, which is expected to be fully operational in 2023.

Selected entities’ compliance with PSPF personnel security requirements was mixed. While most entities had policies and procedures in place for personnel security, some entities were only partially compliant with the PSPF requirements to ensure personnel have appropriate clearances. None of the entities had fully implemented the PSPF requirements introduced in 2014 relating to managing
ongoing suitability. In addition, entities did not always notify AGSVA when clearance holders leave the entity.

**Recommendations (pp.10-11)**

**Recommendation No.1**

The Department of Defence, in consultation with the Attorney-General’s Department, establish operational guidelines for, and make appropriate risk-based use of, clearance maintenance requirements.

Attorney-General’s Department’s response: Agreed.

Department of Defence’s response: Agreed.

**Recommendation No.2**

The Department of Defence implement the Protective Security Policy Framework requirement to obtain explicit informed consent from clearance subjects to share sensitive personal information with sponsoring entities.

Department of Defence’s response: Agreed

**Recommendation No.3**

The Attorney-General’s Department and the Department of Defence establish a framework to facilitate the Australian Government Security Vetting Agency providing sponsoring entities with specific information on security concerns and mitigating factors identified through the vetting process.

Attorney-General’s Department’s response: Agreed.

Department of Defence’s response: Agreed.

**Recommendation No.4**

The Attorney-General’s Department and the Digital Transformation Agency conduct a personnel security risk assessment that considers whether changes are needed to their protective security practices.

Attorney-General’s Department’s response: Agreed.

Digital Transformation Agency’s response: Agreed.

**Recommendation No.5**

The Digital Transformation Agency take immediate action to comply with the Protective Security Policy Framework governance requirements.
ANAO CONCLUSIONS AND RECOMMENDATIONS

Digital Transformation Agency’s response: Agreed.

**Recommendation No.6**

The Attorney-General’s Department, the Australian Securities and Investments Commission, the Department of Home Affairs and the Digital Transformation Agency implement quality assurance mechanisms to reconcile their personnel records with AGSVA’s clearance holder records, and commence clearance processes for any personnel who do not hold a required clearance.

Attorney-General’s Department’s response: Agreed.
Australian Securities and Investments Commission’s response: Agreed.
Department of Home Affairs’ response: Agreed.
Digital Transformation Agency’s response: Agreed.

**Recommendation No.7**

The Attorney-General’s Department, the Australian Radiation Protection and Nuclear Safety Authority, the Australian Securities and Investments Commission and the Digital Transformation Agency review their policies and procedures for eligibility waivers to ensure they are compliant with Protective Security Policy Framework mandatory controls.

Attorney-General’s Department’s response: Agreed.
Australian Radiation Protection and Nuclear Safety Authority’s response: Agreed.
Australian Securities and Investments Commission’s response: Agreed.
Digital Transformation Agency’s response: Agreed.

**Recommendation No.8**

The Attorney-General’s Department, the Australian Radiation Protection and Nuclear Safety Authority, the Australian Securities and Investments Commission, the Department of Home Affairs and the Digital Transformation Agency implement the Protective Security Policy Framework requirement to undertake an annual health check for clearance holders and their managers.

Attorney-General’s Department’s response: Agreed.
Australian Radiation Protection and Nuclear Safety Authority’s response: Agreed.
Australian Securities and Investments Commission’s response: Agreed.
Department of Home Affairs’ response: Agreed.
Digital Transformation Agency’s response: Agreed.

**ANAO Report No.43 (2017-18) Domestic Passenger Screening – Follow-Up**

**Conclusion (pp.8-9)**

As at March 2018, the Department has implemented one and partially implemented four of the five recommendations made in ANAO Audit Report No.5 2016–17, Passenger Security Screening at Domestic Airports (see Table S.1 below). Consequently, while the Department has made progress, it is not yet well placed to provide assurance that passenger screening is effective and that screening authorities comply with the Regulations.

The extent to which the Department has implemented an effective compliance monitoring program has been constrained by the quality of data captured in the Regulatory Management System. Consequently, the ability of the Department to conduct meaningful analysis of compliance activity data and identify non-compliance trends in passenger screening is limited. While the Department has developed a data analysis function to work around the limitations of the Regulatory Management System, its initial analysis was not used to inform planning. The Department has further work to do to be able to identify non-compliance trends and incorporate the results of the analysis into the annual compliance program as recommended in the previous audit.

The Department has developed and approved a learning and development framework. However, the plan to implement the framework has not yet been approved, and a key element yet to be finalised is the approach to monitoring and evaluating the framework. Delivery of appropriate training was delayed by the Department’s decision to broaden the application of the training needs analysis beyond the initial Regulatory Management System focused training recommended by the ANAO (Recommendation No.4) in the previous audit. While steps were taken to address short-term training needs, the first training courses outlined in the learning and development framework commenced in February 2018.

The Department has developed, but not yet implemented performance monitoring arrangements despite numerous reports including ANAO Audit Report No.26 2002–03, Aviation Security in Australia recommending that performance measures be implemented. Most recently, the timely implementation of these performance measures has been impacted by the Department’s decision to implement the
measures in July 2018 as part of the broader Enhanced Mandatory Reporting Project. While the Department has made progress to improve the reporting provided to its stakeholders, the ability of the Department to accurately assess the effectiveness of passenger screening is limited due to the quality of the data captured in the Regulatory Management System, the lack of an associated reporting function and because performance measures have not yet been implemented.

**Recommendations (p.11)**

**Recommendation No.1**

In implementing Recommendation No.2 from the previous audit, the Department should ensure that its approach delivers a meaningful analysis of passenger screening compliance activities and outcomes. The analysis should: be capable of accurately identifying non-compliance trends; generate results that are used to inform the development of the risk and compliance prioritisation ratings; and be incorporated into subsequent compliance monitoring programs.

Department of Home Affairs response: Agreed.

**Recommendation No.2**

In implementing Recommendation No.4 from the previous audit, the Department should develop and implement a monitoring and evaluation strategy, so it can assess to what extent the objectives of the learning and development framework are being met.

Department of Home Affairs response: Agreed.

**Recommendation No.3**

In implementing Recommendation No.3 from the previous audit, the Department should ensure that performance measures are established in a timely manner alongside an effective monitoring and review mechanism to provide assurance that the performance measures developed for passenger screening are practical, achievable and measurable.

Department of Home Affairs response: Agreed.
## C. Submissions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Australian Securities and Investments Commission</td>
</tr>
<tr>
<td>2</td>
<td>Australian Radiation Protection and Nuclear Safety Agency</td>
</tr>
<tr>
<td>3</td>
<td>Attorney-General’s Department</td>
</tr>
<tr>
<td>4</td>
<td>Digital Transformation Agency</td>
</tr>
<tr>
<td>5</td>
<td>Department of Home Affairs</td>
</tr>
<tr>
<td>6</td>
<td>Department of Defence</td>
</tr>
<tr>
<td></td>
<td>▪ 6.1 Supplementary to submission 6</td>
</tr>
<tr>
<td></td>
<td>▪ 6.2 Supplementary to submission 6</td>
</tr>
<tr>
<td></td>
<td>▪ 6.3 Supplementary to submission 6</td>
</tr>
<tr>
<td>7</td>
<td>Australian National Audit Office</td>
</tr>
<tr>
<td></td>
<td>▪ 7.1 Supplementary to submission 7</td>
</tr>
<tr>
<td>8</td>
<td>Department of Home Affairs</td>
</tr>
<tr>
<td></td>
<td>▪ 8.1 Supplementary to submission 8</td>
</tr>
<tr>
<td>9</td>
<td>Edward Barker</td>
</tr>
</tbody>
</table>
D. Public Hearings

Wednesday, 17 August 2018

Committee Room 2R1, Parliament House, Canberra

*Australian Radiation Protection and Nuclear Safety Authority*

Dr Gillian Hirth, Deputy Chief Executive Officer and Chief Radiation Health Scientist

Ms Julie Murray, Director, Facility Safety and Agency Security Adviser

*Australian Securities and Investments Commission*

Mr Carlos Iglesias, Chief of Operations

Mr Sean Powe, Agency Security Adviser

*Attorney-General’s Department*

Ms Sarah Chidgey, Acting Deputy Secretary, Integrity and International Group

Ms Helen Daniels, Assistant Secretary, Human Resources

*Department of Home Affairs*

Mr Angus Kirkwood, Acting First Assistant Secretary, Aviation & Maritime Security Division

*Australian National Audit Office*

Mr Grant Hehir, Auditor-General

Ms Deborah Jackson, Executive Director, Performance Audit Services Group

Ms Lisa Rauter, Group Executive Director, Performance Audit Services Group

Mr Daniel Whyte, Senior Director, Performance Audit Services Group
Department of Defence

Mr Daniel Fortune, Assistant Secretary, Vetting

Department of Home Affairs

Mr Mark Brown, Acting First Assistant Secretary, Integrity Security and Assurance Division

Ms Belinda Gill, Acting Assistant Secretary, Audit and Assurance Branch

Digital Transformation Agency

Mr George-Philip de Wet, Chief Operating Officer

Wednesday, 19 September 2018

Committee Room 2R1, Parliament House, Canberra

Australian National Audit Office

Mr Grant Hehir, Auditor-General

Ms Sally Ramsey, Executive Director, Performance Audit Services Group

Ms Joyce Knight, Senior Director, Performance Audit Services Group

Department of Home Affairs

Mr Angus Kirkwood, Acting First Assistant Secretary, Aviation & Maritime Security Division

Mr Richard Farmer, Assistant Secretary, Aviation & Maritime Security Division
Tuesday, 12 February 2019

Committee Room 2R1, Parliament House, Canberra

*Australian National Audit Office*

Mr Grant Hehir, Auditor-General

Ms Deborah Jackson, Executive Director, Performance Audit Services Group

Ms Lisa Rauter, Executive Director, Performance Audit Services Group

Mr Daniel Whyte, Senior Director, Performance Audit Services Group

*Department of Defence*

Mr Daniel Fortune, Assistant Secretary, Vetting